UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA	**CASE NOS.: 5:18-CR-448**
Plaintiff	**JUDGE BENITA Y. PEARSON**
v.	**MOTION TO COMPEL**
PHILIP M. POPA, JR.,	
Defendant	

Now comes the Defendant Philip M. Popa, Jr., by and through the undersigned counsel, and hereby moves this Court to Order the Government to produce information regarding Freenet software, which is the computer software program utilized by the Government during the course of its investigation of Mr. Popa. Mr. Popa makes this Motion pursuant to Federal Rules of Criminal Procedure Rule 16 in addition to *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972) and the Fifth, Sixth and Fourteenth Amendments to the United States Constitution. The items requested constitute documents or data that is material to preparing a defense against the Government's case-in-chief at trial. This Motion is supported by the Memorandum in Support, which is attached hereto and incorporated herein by express reference.

Respectfully submitted,
WILLIAM T. WHITAKER CO. LPA

/s/Andrea Whitaker
ANDREA WHITAKER #0074461
54 E. Mill Street Suite 301
Akron, Ohio 44308
T: 330-762-0287 F: 330-762-2669
whitaker@whitakerlawlpa.com
Attorney for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was electronically filed this 6th day of February, 2019. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system.

/s/ Andrea Whitaker
Andrea Whitaker

MEMORANDUM IN SUPPORT

I. FACTS

Defendant, John Popa, is charged with one count receipt of visual depictions of real minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2) and one count of possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The Government's discovery response and Affidavit in Support of the Search Warrant refer to Freenet as the computer software program used by law enforcement.

On July 17, 2018, Ryan D. Anschutz, a Task Force Officer in the Federal Bureau of Investigation applied for a search warrant to search and seize evidence at 533 Redwood St SW, Beach City, Ohio 44608. See Search Warrant and Affidavit attached hereto as Exhibit A. The request for a warrant was supported by an affidavit signed by Agent Anschutz. In the affidavit, the Affiant (Agent Anschutz) avers that there is probable cause to believe that a user of an IP address at this address has received, possessed, and/or distributed child pornography. Ex., A, Affidavit in Support of Search Warrant ("Affidavit"), ¶ 3. The Affidavit contains the Affiant's experience, a description of the place to be searched and the items to be seized, and definitions of terms contained there.

The Affidavit also contains an explanation of "Freenet." According to the Affiant, it is "an Internet-based, peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network." Ex. A, Affidavit, ¶7. The Affiant further explains that in "order to access Freenet, a user must first download the Freenet software, which is free and publicly available. The Freenet 'source code" - i.e., the computer programming code that facilitates Freenel's operation - is also publicly available. In other words, Freenet is 'open source" software that may be examined and analyzed by anyone with the pertinent expertise or

knowledge." Id. at ¶ 8. The Affidavit then goes on to explain a Freenet user may be an "original requestor" of a file or one that "is merely forwarding the request of another user." Id. at ¶ 12.

This fact, and the Affiant's knowledge of it, is of the upmost importance because it indicates that some "requests" for files, including child pornography, happen without the users knowledge or consent. The Affiant recognizes that law enforcement must be able to distinguish between the two types of requests in order to identify where there is probable cause that a user is requesting illegal material. Id.

In fact, "Freenet attempts to hide which computer uploaded a file into or downloaded a file from the network by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (Le., the peer was the "original requestor" of the file), or whether that peer was simply forwarding a different peer's request." Id. at ¶ 14. "Freenet attempts to hide the identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file." Id.

According to the Affidavit, a "modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations." Id. at ¶ 20. Using that modified version of Freenet, in April, 2018 , Agent Anschutz identified "a computer running Freenet software, with an IP address of 173.90.126.69, with 13.1 peers, requested from a law enforcement computer 136 out of 1786 total pieces needed to assemble a file with a SHA1 digital hash value of ATLOOVASIDQV6JPNOK4Z3MTKWGYFYS6W." Affidavit, ¶ 27. In other words, the computer at the suspect IP address reportedly requested less than .075% of a file. Officer

Anschutz then downloaded the completed file from another source and described the completed file in the Affidavit. Id. This activity occurred for several additional files. Id. at ¶¶ 28-29.

The Affidavit then indicates that "[u]sing publicly available search tools, law enforcement determined that IP address 173.90.126.69 was controlled by Internet Service Provider ("ISP') Time Warner Cable." Id. at 32. The Affiant then issued an administrative subpoena sent "Time Warner Cable for the date and times that the above-described files were downloaded" and found that the "IP address was assigned to the account registered to 'James Skelly,' at the PREMISES, email addresswowsaddie@twc.com. Telephone number 330-324-4421, account number 206389203 and the active IP address date of 12119/2017." Id. at 33

Thereafter, Agent Anschutz prepared the Affidavit in support of his request for a search warrant on July 17, 2018. The Affidavit was submitted to and approved by a Magistrate Judge of the United States District Court for the Northern District of Ohio that same day. On July 17, 2018, law enforcement officers executed the search warrant at Mr. Popa's residence and seized several items, which were subsequently forensically analyzed by law enforcement agents. Law enforcement officers also arrested and obtained a statement from Mr. Popa.

As a result of the Government's investigation in this case, Mr. Popa was indicted on August 14, 2018 with the foregoing offenses. After receiving the Government's initial discovery response, defense counsel retained the services of a local expert at defense counsel's expense. Consultation with the expert and a review of the discovery identified several issues for pretrial motions. However, the expert had little experience with Freenet. Mr. Popa's counsel requested a copy of the law enforcement modified version of Freenet. The Government indicated that the law enforcement software was not discoverable.

As the undersigned was preparing the pretrial motions, she was referred to Tami Loehrs of Loehrs Forensics, L.L.C. as someone with potentially more experience with Freenet. The undersigned immediately contacted Ms. Loehrs and provided her with a copy of the discovery to determine if additional issues were significant to Mr. Popa's defense. Ms. Loehrs reviewed the discovery and provided an Affidavit of her initial findings. See Affidavit of Tami Loehrs (TL Affidavit") attached hereto as Exhibit B. Ms. Loehrs identified several issues heretofore unknown to the undersigned and indicated that it would be necessary to conduct an independent forensic examination of the electronic evidence that was seized in connection with the search warrants. Ms. Loehrs has extensive experience conducting forensic examinations in child pornography cases and is acutely familiar with the investigative aspects of such cases, including the Government's use of proprietary investigative software. Simultaneously with the filing of this Motion, Mr. Popa is filing a Motion to Suppress, with leave to supplement, and a Motion to Appoint Ms. Loehrs as an expert for Mr. Popa.

Based upon her review of the discovery as well as her prior experience with law enforcement's use of modified software programs, Ms. Loehrs opines that an independent forensic examination of the law enforcement version of the Freenet Software is necessary in order to determine the validity and/or reliability of the Government's forensic evidence and to assess the information provided in the Affidavit in support of the search warrant. As she notes, in her "forensic training, some of which has come directly from law enforcement, [she has] been taught that [she] cannot rely on a tool (software) that has not been properly tested and validated by [her] and is not available for testing and validation by [her] industry peers." TL Aff., ¶ 21. Ms. Loehrs, however, goes farther than to just note that it is best practice, as noted herein, she identifies specific concerns regarding the law enforcement Freenet that require an independent analysis.

Specifically, Ms. Loehrs notes that she has "worked on hundreds of cases throughout the country involving law enforcement's investigations of P2P and BitTorrent file sharing networks, including the use of Freenet, which has brought to light serious issues with regard to the accuracy and reliability of the proprietary software used by law enforcement to conduct these investigations and whether that software is going beyond information that is publicly available as well as reporting false information regarding files that do not exist on a suspect computer and/or do not contain child pornography." TL Aff, ¶ 7. She is concerned that, in "spite of this, Officer Anschutz avers in his Affidavit that the IP address associated with Mr. Popa contains child pornography based on incomplete files reported by his law enforcement tool and then describes completed files that he downloaded from other sources." Id. at 15.

Agent Anschutz refers to the "law enforcement's tool" used to analyze the network and an allegedly peer reviewed article that allow him to come to the conclusion that is significantly more probable than not that the suspect IP address was the original requestor of the child pornography files. "However, Officer Anschutz provides no information regarding "law enforcements tool", including whether that tool has been tested and validated, nor does he provide any log files created by the law enforcement tool as foundation for his opinions." T.L. Aff, ¶ 16. Moreover, the Affiant refers to a "peer-reviewed, publicly-available academic paper describing the methodology of that mathematical formula." Affidavit, ¶ 24. While the Government has provided the paper to the undersigned, there has been no response to the request for evidence that the paper was peer-reviewed. The undersigned has been unable to locate any such review in her own research.

As noted by Ms. Loehrs, "it is critical to Mr. Popa's defense to understand how law enforcement's proprietary tool functions in order to determine its reliability and accuracy in identifying files that Officer Anschutz claims originated from Mr. Popa's IP address." Id. at ¶ 17.

She also refers to logs created by "law enforcement's proprietary tools" documenting activity "which could be analyzed to corroborate or refute Officer Anschutz's conclusions." Id. at 16. Additionally, Freenet "creates detailed logs of activity that could be analyzed to corroborate or refute Officer Anschutz's conclusions although no Freenet logs." Id. To date, no such logs have been produced. However, to be fair, until the undersigned spoke to Ms. Loehrs, she was not aware that such logs existed to be able to request them.

As the foregoing information establishes, counsel has requested the law enforcement version of Freenet and has been told that it is not discoverable. The Government indicates that they will not provide software as requested. For the reasons that follow, Mr. Popa respectfully requests that this Honorable Court issue an Order compelling the Government to disclose and/or produce this forthwith. Upon receipt, Mr. Popa will then request that the Government make available the computer seized in July of 2018 for Ms. Loehrs to conduct an independent forensic analysis.

II. LAW AND ARGUMENT

Rule 16 of the Federal Rules of Criminal Procedure states that a criminal defendant has the right to inspect all documents, data, or tangible items within the Government's "possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim.P. 16(a)(1)(E). Evidence is "material" if it is "helpful" to the development of a possible defense. *See United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995); *see also United States v. Dobbins*, 482 Fed. Appx. 35, 41 (6th Cir. 2012). In *Brady v. Maryland*, 373 U.S. 83, 87 (1963), the United States Supreme Court ruled that the suppression by the prosecution of evidence favorable to the accused, upon request for disclosure by the accused, violates due process. The Supreme Court further expanded an accused's right to evidence held by the Government in *Giglio v. United States*, 405 U.S. 150

(1972), to include evidence that could be used to impeach Government witnesses. Pursuant to Rule 16, *Brady* and *Giglio*, the Government is required to produce the requested information regarding Freenet because it is material to the development of a defense in this case and is necessary in order to effectively cross-examine the Government's witnesses at trial.

Agent Anschutz used the law enforcement version of the Freenet software to identify an IP address that was alleged to have requested child pornography materials from other Freenet users. He then used the software to download files from other users on Freenet based upon hash values that were reported from the suspect IP address.

As the foregoing establishes, the Freenet software is a critical component of the Government's case-in-chief. Moreover, all evidence relied upon to obtain the search warrant – including the issuance of the Administrative Subpoena to Time Warner Cable as well as the Affidavit in support of the search warrant – was a product of the Freenet software. To the extent that the Freenet software erroneously claimed to find that there was child pornography on Mr. Popa's computer or from his IP address, law enforcement agents violated Popa' Fourth Amendment rights. Assuming this is established, all evidence seized in connection with this investigation would be subject to suppression. This puts directly at issue the use of the law enforcement version of Freenet to obtain access to Popa' computer.

The flaws identified by Ms. Loehrs in her Affidavit in Freenet would be "material" to preparing the defense, including pretrial motions, *see* Fed. R. Crim. P. 16(a)(1)(E), and therefore subject to disclosure by the Government. *See United States v. De Los Santos*, 810 F.2d 1326, 1330 (5th Cir. 1987)(holding that evidence is "material" when it would be helpful to the defense in preparing for trial). These deficiencies would similarly be considered exculpatory and, thus, subject to disclosure under *Brady*, *supra*.

In *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), the Ninth Circuit Court of Appeals overruled the district court's refusal to Order the disclosure of discovery relating to a similar FBI-run computer program in a child pornography distribution case. *Id*. at 1107. Budziak filed a Motion to compel the discovery of the technical specifications of the software program as well as access to a copy of the installable software for an independent forensic review. After these requests were denied, the agents were permitted to testify concerning their investigation, including their utilization of the aforementioned software. *Id*. at 1108. On appeal, the Ninth Circuit remanded the case back to the district court holding that Budziak had made the requisite showing that such information was material to his defense of the case: "[g]iven that the distribution charge against Budziak was premised on the FBI's use of the EP2P program to download files form him, it is logical to conclude that the functions of the program were relevant to his defense." *Id*. at 1112.

Further, in order to effectively cross-examine Agent Anschutz on the reliability and functionality of the law enforcement Freenet software, defense counsel must be provided access to the software. In *Budziak, supra*, the Ninth Circuit explained that "access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Budziak*, 697 F.3d at 1112. In this regard, it was not sufficient that the defendant had the ability to cross-examine the agent at trial because he was denied the "background material on the software that could have enabled him to pursue a more effective examination." *Id*. The Ninth Circuit found that "a party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately." *Id*., *citing United States v. Liebert*, 519 F.2d 542, 547-48 (3rd Cir. 1975) and *United States v. Dioguardi*, 428 F.2d 1033, 1038 (2nd Cir. 1970)("[i]t is quite incomprehensible

that the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and use on cross-examination if desired").

Recent decisions from other jurisdictions provide further support for the proposition that when a Government investigation involves the use of computer software to obtain a search warrant and eventual Indictment, defendants should be afforded access to the software and its specifications. *See, e.g.*, *United States v. Todd Hartman*, 8:15-cr-00063 (U.S. D.C. CA 2015) (doc. 87); *United States v. John Crow*, 1:11-cr-01690 (U.S. D.C. N.M. 2013) (doc. 88); *United States v. Angel Ocasio*, 3:11-cr-02728 (U.S. D.C. W.D. TX 2013) (doc. 150).

In the case at bar, the defense has specifically articulated concerns regarding the operation of the Freenet software and its ability to identify if illegal material was obtained by a particular IP address. Concerns regarding the reliability and functionality of the software are also raised by the information provided in the discovery materials as identified in Ms. Loehrs' Affidavit. Mr. Popa is not obligated to merely rely upon the Government's representations concerning the reliability and/or functionality of the software or that his own separate investigation would be unfruitful. *See Budziak*, 697 at 1113.

Because Mr. Popa has made a sufficient showing regarding the relevance and helpfulness of the discovery materials requested herein at issue, this Court must therefore balance the public's interest in protecting the flow of information against the defendant's right to prepare his or her defense. *United States v. Whitney*, 633 F.2d 902, 911 (9th Cir.1980); *Roviaro v. United States*, 353 U.S. 53, 62 (1957) ("[w]hether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the [undisclosed evidence], and other relevant factors").

The facts and circumstances of this case are identical to those at issue in *Budziak*, *supra*. In order to assess the reliability and functionality of the Freenet software, assess pretrial motions and effectively cross-examine Agent Anschutz, the defense must be permitted access to the program itself. This is especially crucial when the charges "against the defendant [are] predicated largely on computer software functioning in the manner described by the Government, and the Government is the only party with access to that software." *Budziak*, 697 F.3d at 1113. Agent Anschutz use of the law enforcement version of Freenet has put the software directly at issue.

III. CONCLUSION

Based upon the foregoing analysis, as well as additional evidence and arguments to be presented at a hearing on this matter, the undersigned submits that they are entitled to the materials heretofore requested concerning the software that was utilized by law enforcement in connection with this case. Accordingly, Mr. Popa respectfully requests that this Honorable Court issue an Order compelling the Government to provide defense counsel with the following materials and/or items forthwith:

- Any and all log files created by the law enforcement software utilized by Officer Anschutz in his investigation of Freenet for the date of April 21, 2018;
- An installable copy of the law enforcement software utilized by Officer Anschutz in his investigation of Freenet for the date of April 21, 2018 for testing and validation or, in the alternative, documentation of testing and validation of the law enforcement software by a qualified third party;
- Forensic images of all electronic evidence seized from Mr. Popa for independent examination by Loehrs Forensics to be made available at the FBI facility in Phoenix, Arizona.

WHEREFORE, Defendant Popa, hereby respectfully requests that this Honorable Court issue an Order compelling the Government to produce and provide the above-referenced materials to defense counsel.

Respectfully submitted,
WILLIAM T. WHITAKER CO. LPA

/s/Andrea Whitaker
ANDREA WHITAKER #0074461
54 E. Mill Street Suite 301
Akron, Ohio 44308
T: 330-762-0287 F: 330-762-2669
whitaker@whitakerlawlpa.com
Attorney for Defendant